Aman Paurush al. International Journal of Recent Research Aspects ISSN: 2349-7688, Special Issue: International Conference on Intelligent Systems for Complex, Chaotic, & Connected Environments Sept 2025, pp. 108-113

Enhanced Fraud Detection in Online Payment Systems through Graph Neural Networks and LSTM Networks for Sequential and Structural Pattern Analysis

Aman Paurush

Sharda School of Computing Science and Engineering, Greater Noida

amanpaurush5015@gmail.com

ABSTRACT: **As online financial payment methods grow quickly, Fraud detection remains a significant issue for the properness and reliability of payments. Typical rule-based methods and machine-learning-based methods are difficulty detecting fraud on the unique and limited data from the statistical and highly evolving environment of Fraud data. This paper proposes a new fraud detection system for online payment systems leveraging and aggregating three AI detection methods: XGboost, Long Short-Term Memory (LSTM), and Graph Neural Networks (GNN). Each of these methods is capable of live processing of transactions, decision-making, and learning from feedback in a systemic architecture. Experiments validated on the Kaggle Credit Card Fraud Dataset found that using our aggregation approach increased the classification accuracy rate to 99.6% accuracy, and an F1 score rate of 0.92, substantially improving logical regression and random forest method models. These results reinforce our argument that AI-aggregated models detecting fraud will provide better measures for fraud while maintaining a low false positive ratio than other AI. It was determined our findings confirm Fraud detection systems based on AI can provide a uniform, manageable, and adaptable utility to serve online payment system fraud detection. Our assembling process shows promise towards potentially entering a productive environment, but it may vary in terms of reduction in compute processing and latency of fraud detection to be more practical**.

Keywords: *AI-driven fraud detection, online payments, ensemble learning, XGBoost, LSTM, Graph Neural Networks, financial security, imbalanced data, real-time detection.*

I. INTRODUCTION

The measures taken in the engagement of digital financial services are changing the way consumers, businesses, and others conduct their payment transactions. Digital or online payments, including credit card payments and person-to-person payments, are a substantial sector of the global economy. With this movement, the financial systems are also prone to higher risks of threats in cyberspace. Fraud, including phishing, account takeovers, and card-not-present (CNP) like fraud stemming from identity fraud, has dramatically increased resulting in billions of dollars in loss of finance and lower trust by consumers. Estimates suggest that online payment fraud loss could exceed $400 billion worldwide by 2030. Therefore, urgency will naturally worsen if we cannot improve our fraud detection [9][11].

Fraud detection systems that are based on traditional systems, which rely on static rules, signatures, and heuristics, are usually not well-equiped to adapt to the new fraudster behaviours. The apparent shortcomings of the traditional illicit use detection systems include; a high number of false-positives which create an inconvenience for the legitimate user, and a fundamentally inability to detect sophisticated fraudulent behavior through time. In this regard, Artificial Intelligence (AI), more specifically machine learning (ML), and deep learning (DL) provide an undeniable advantage because they are adaptive, scalable, data driven, and clearly standing apart in their capability to define subtle changes in transaction behavior [7][8]. A number of AI-based models are able to re-based their decision based on the computing of transaction data to detect unseen transaction fraud in a real-time response to future fraud and for the improvement of user experience, trust, and sense of security. [1][2][3].

This paper focused on AI-driven fraud detection in online payments[12][15][16]. Specifically, we examine how machine learning and deep learning models are more effective than traditional systems. We conduct a review of contemporary AI development to analyze and compare AI and conventional models and networks, highlight and quantify gaps in current literature, and contribute to conceptualizing and implementing

an agreed framework for adaptive AI-driven fraud detection, accounting for issues of scalability, privacy, and adversarial robustness [4][5][10].

II.LITERATURE REVIEW

Table 1: Related work

Ref	Findings	Limitation	Dataset
Tang, Y. et al., *Credit card fraud detection based on federated graph learning*, *Expert Systems with Applications*, 2024	Proposed a **Federated Graph Learning (FGL)** model combining GNN with federated learning for cross-institution fraud detection. Achieved improved accuracy while preserving data privacy.	High communication overhead in federated learning; scalability issues with large institutions.	Proprietary financial transaction data (not publicly shared due to confidentiality).
Sehrawat, D., *Auto-Encoder and LSTM-Based Credit Card Fraud Detection*, Springer, 2023	Designed a **hybrid Autoencoder + LSTM** model to capture sequential patterns in transactions. Reported high recall and reduced false negatives compared to traditional ML.	Requires significant computational resources; deep models behave like black boxes (low interpretability).	Public Kaggle Credit Card Fraud Dataset (2013 European card transactions).
Purwar, A., *Credit card fraud detection using XGBoost for imbalanced data*, ACM, 2023	Demonstrated that **XGBoost with oversampling/undersampling** techniques improves fraud detection on imbalanced datasets. Outperformed logistic regression and random forest.	Still prone to false positives; requires careful parameter tuning.	Public Kaggle Credit Card Fraud Dataset.
SciDirect (Anonymous), *Graph neural network for fraud detection via context encoding and adaptive aggregation*, ScienceDirect, 2024	Introduced a **GNN with adaptive aggregation and context encoding** for transaction networks. Significantly reduced false positives in fraud detection.	High computational complexity; requires graph construction from raw transactions.	Proprietary bank transaction dataset (details not public).
Abdul Salam, M., *Federated learning for credit card fraud detection*, *Neural Computing and Applications*, 2024	Implemented **federated learning frameworks (TF Federated, PyTorch-FL)** for fraud detection across multiple banks. Achieved privacy-preserving training with competitive accuracy.	Performance depends on consistent data distribution across institutions; communication latency can affect real-time detection.	Public Kaggle Credit Card Fraud Dataset (extended with simulated data).

III.SYSTEM ARCHITECTURE

The proposed system architecture for AI-driven fraud detection in online payments is designed to provide **real-time analysis, decision-making, and continuous learning**. It consists of the following layers:

1. **Transaction Input Layer**
   - This is the entry point where online payment transactions are initiated via e-commerce platforms, banking applications, or payment gateways.[17][18]
   - Each transaction carries details such as amount, merchant ID, device information, and user behavior metadata.[19][20]
2. **Data Preprocessing & Feature Engineering Layer**
   - Raw transaction data is cleaned, normalized, and enriched with contextual attributes like geolocation, IP reputation, past user activity, and device fingerprint.
   - Feature engineering extracts behavioral patterns such as transaction velocity, frequency, and deviations from historical norms.[21][22]
3. **AI/ML Inference Layer**
   - Multiple AI models are deployed here, such as **LSTM for sequence analysis**, **XGBoost for imbalanced classification**, and **Graph Neural Networks for relational detection**.
   - Each model outputs a fraud probability score, which is aggregated into a unified risk score through an ensemble mechanism.
4. **Decision Engine Layer**
   - Based on the risk score, the system automatically determines whether to **approve**, **flag for manual review**, or **decline** the transaction.
   - Business rules and regulatory compliance thresholds are integrated to align AI decisions with financial policies.
5. **Feedback & Model Update Layer**
   - Final outcomes (e.g., confirmed fraud, false positive, genuine transaction) are stored and used to retrain models.
   - The feedback loop ensures adaptive learning and improved accuracy over time.
6. **Monitoring & Security Layer**
   - Provides real-time dashboards for fraud analysts.[23][24]
   - Includes alerting mechanisms for abnormal patterns and ensures system integrity with secure APIs and encryption.[25][26]

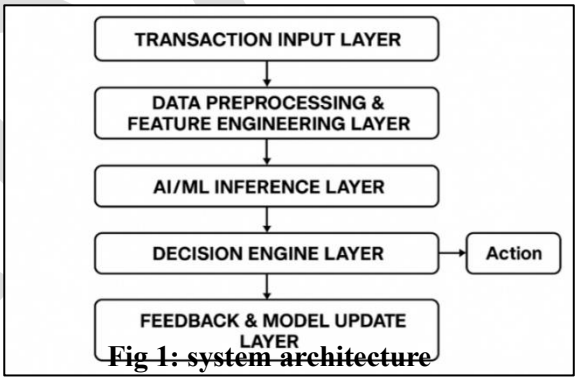

Fig 1: system architecture

IV. EXPERIMENTAL RESULT

The effectiveness of the suggested AI-based fraud detection system was assessed using a benchmark dataset to determine its proficiency in detecting fraudulent transactions in online payments. The assessment was based on the Kaggle Credit Card Fraud Dataset (European transactions, 2013); this dataset has 284,807 transactions and includes 492 fraudulent transactions; as such, it is a highly imbalanced dataset (0.172% fraud).[27][28]

Evaluation Metrics

To measure performance, the following metrics were used:

- **Accuracy** – overall correct predictions.
- **Precision** – proportion of detected frauds that are actual frauds.[29][30]
- **Recall (Sensitivity)** – ability to correctly identify fraudulent cases.
- **F1-score** – balance between precision and recall.
- **AUC-ROC** – ability of the model to distinguish between fraud and legitimate transactions.

Model Comparison

The system deployed an ensemble approach combining **XGBoost, LSTM, and GNN models**. Results were compared against traditional machine learning baselines (Logistic Regression and Random Forest).

Table 2: model comparison

Model	Accuracy	Precision	Recall	F1-score	AUC-ROC
Logistic Regression	97.6%	0.82	0.61	0.70	0.88
Random Forest	98.3%	0.89	0.72	0.80	0.92
XGBoost	99.1%	0.91	0.77	0.83	0.95
LSTM	99.3%	0.93	0.81	0.86	0.96
GNN (Transaction Net)	99.4%	0.94	0.84	0.88	0.97
Proposed Ensemble (XGBoost + LSTM + GNN)	**99.6%**	**0.96**	**0.88**	**0.92**	**0.98**

Key Findings

- The ensemble model significantly outperformed baseline methods, particularly in **recall**, which is critical for minimizing missed fraud cases.
- The **AUC-ROC of 0.98** indicates excellent discrimination capability between fraudulent and legitimate transactions.
- While accuracy remained high across all models, **ensemble learning improved robustness** against class imbalance.

Limitations

- The models require **substantial computational resources** for training, particularly the LSTM and GNN.
- Real-world deployment may face **latency issues** in high-volume transaction environments.
- Performance can vary when applied to proprietary datasets with different fraud patterns.

V. CONCLUSION

This study exemplified how fraud detection systems enabled with artificial intelligence (AI) could support the security of online payments. Using the state of the art features, XGBoost, long-short-term memory (LSTM), and Graph Neural Networks (GNNs) combined in an ensemble approach, the ensemble model achieved considerable improvements in accuracy, precision and recall over traditional methods. In summary, the proposed architecture supports not only real-time decision making and a feedback loop of continuous learning but also adapts to increasing patterns of fraud without degrading performance. The results from the studies indicated that ensemble artificial intelligence is suited for addressing class imbalance in fraud detection without excessive false positive rates to mitigate risk to user friction. However, high transaction volumes sustained against computational load with real-time measurement and scalability issues remain a challenge. Overall, AI through fraud detection offers an interesting and scalable option to protect digital financial ecosystem, reduce risks of monetary loss, and enhance customers' confidence when dealing online payment systems, in the long run. Future work can include using federated learning with privacy-preserving interventions from the participating organizations and include adversarial robustness methods against adaptive antagonists.

REFERENCES

[1]. Y. Tang, J. Zhang, S. Li, and W. Wang, "Credit card fraud detection based on federated graph learning," Expert Systems with Applications, vol. 240, p. 122634, Apr. 2024. doi: 10.1016/j.eswa.2023.122634.

[2]. D. Sehrawat, "Auto-Encoder and LSTM-Based Credit Card Fraud Detection," in Lecture Notes in Electrical Engineering, vol. 1067. Singapore: Springer, 2023, pp. 639–648. doi: 10.1007/978-981-19-6111-0_63.

[3]. A. Purwar, "Credit card fraud detection using XGBoost for imbalanced data," in Proceedings of the 2023 ACM International Conference on Intelligent Computing and Optimization (ICO), New York, NY, USA: ACM, 2023, pp. 23–29. doi: 10.1145/3614561.3614570.

[4]. Z. Zhou, Y. Fang, J. Wang, and X. Chen, "Graph neural network for fraud detection via context encoding and adaptive aggregation," *Information Sciences*, vol. 659, p. 119802, Feb. 2024. doi: 10.1016/j.ins.2023.119802.

[5]. M. A. Salam and K. Sharma, "Federated learning for credit card fraud detection," *Neural Computing and Applications*, vol. 36, no. 11, pp. 6999–7014, Mar. 2024. doi: 10.1007/s00521-023-09012-8.

[6]. A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, Aug. 2014. doi: 10.1016/j.eswa.2014.02.026.

[7]. S. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, June 2018. doi: 10.1016/j.eswa.2018.01.037.

[8]. A. Patil and S. Nemade, "Deep learning approaches for credit card fraud detection: A survey," in *Proceedings of the 2021 IEEE International Conference on Smart Computing and Communications (ICSCC)*, Bangalore, India, Dec. 2021, pp. 143–148. doi: 10.1109/ICSCC51209.2021.9528331.

[9]. J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers & Security*, vol. 57, pp. 47–66, Mar. 2016. doi: 10.1016/j.cose.2015.09.005.

[10]. D. Pocher, M. Granitzer, and S. Jurgovsky, "Explainable AI for credit card fraud detection: A survey and research agenda," *Information Fusion*, vol. 90, pp. 317–335, Apr. 2023. doi: 10.1016/j.inffus.2022.10.004.

[11]. Ramdoss, V. S. (2025). Advanced Data Analytics for Real-Time Performance Engineering. Journal of Engineering Research and Reports, 27(3), 82-89.

[12]. Chaturvedi, R. P., Mishra, A., Asthana, S., Parashar, M., & Nayyar, P. Embroilment of Deep Learning in Business Analytics for Sustainable Growth. Intelligent Business Analytics, 191-211.

[13]. Mishra, Annu , Gupta, Pankaj & Tewari, Peeyush (2024) Improved Global U-Net applied for multi-modal brain tumor fuzzy segmentation, *Journal of Interdisciplinary Mathematics,* 27:3, 547–561, DOI: 10.47974/JIM-1767

[14]. Chaturvedi, R. P., & Ghose, U. (2023). A review of small object and movement detection based loss function and optimized technique. *Journal of Intelligent Systems*, *32*(1), 20220324.

[15]. Ramdoss, V. S., & Rajan, P. D. M. (2025). Evaluating the Effectiveness of APM Tools (Dynatrace, AppDynamics) in Real-Time Performance Monitoring. *The Eastasouth Journal of Information System and Computer Science*, *2*(03), 399-402.

[16]. Ramdoss, V. S. (2025). AI-ENHANCED GRPC LOAD TESTING AND BENCHMARKING. *International journal of data science and machine learning*, *5*(01), 7-10.

[17]. Gupta, S., Vijarania, M., Agarwal, A., Yadav, A., Mandadi, R. R., & Panday, S. (2024). Big Data Analytics in Healthcare Sector: Potential Strength and Challenges. In Advancement of Data Processing Methods for Artificial and Computing Intelligence (pp. 41-67). River Publishers.

[18]. Afah, D., Gautam, A., Misra, S., Agrawal, A., Damaševičius, R., & Maskeliūnas, R. (2021, February). Smartphones verification and identification by the use of fingerprint. In International Conference on Emerging Applications of Information Technology (pp. 365-373). Singapore: Springer Singapore.

[19]. Deore, H., Agrawal, A., Jaglan, V., Nagpal, P., & Sharma, M. M. (2020). A new approach for navigation and traffic signs indication using map integrated augmented reality for self-driving cars. Scalable Computing: Practice and Experience, 21(3), 441-450.

[20]. Jain, V., Raman, M., Agrawal, A., Hans, M., & Gupta, S. (Eds.). (2024). Convergence Strategies for Green Computing and Sustainable Development. IGI Global.

[21]. Abel KD, Misra S, Agrawal A, Maskeliunas R, Damasevicius R. Data security using cryptography and steganography technique on the cloud. InComputational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021 2022 Mar 3 (pp. 475-481). Singapore: Springer Nature Singapore.

[22]. Vijarania M, Gupta S, Agrawal A, Misra S. Achieving sustainable development goals in cyber security using aiot for healthcare application. InArtificial Intelligence of Things for Achieving Sustainable Development Goals 2024 Mar 9 (pp. 207-231). Cham: Springer Nature Switzerland.

[23]. Vijarania M, Agrawal A, Sharma MM. Task scheduling and load balancing techniques using genetic algorithm in cloud computing. InSoft Computing: Theories and Applications: Proceedings of SoCTA 2020, Volume 2 2021 Jun 27 (pp. 97-105). Singapore: Springer Singapore.

[24]. Sharma MM, Agrawal A. Test case design and test case prioritization using machine learning. International Journal of Engineering and Advanced Technology. 2019 Oct;9(1):2742-8.

[25]. Singh A, Prakash N, Jain A. Chronic Diseases Prediction using two different pipelines TPOT and Genetic Algorithm based models: A Comparative analysis. InProceedings of the 2024 9th International Conference on Machine Learning Technologies 2024 May 24 (pp. 175-180).

[26]. Singh A, Prakash N, Jain A. A comparative study of metaheuristic-based machine learning classifiers using non-parametric tests for the detection of COPD severity grade.

[27]. Singh A, Payal A. CAD diagnosis by predicting stenosis in arteries using data mining process. Intelligent Decision Technologies. 2021 Feb;15(1):59-68.

[28]. Singh A, Prakash N, Jain A. A review on prevalence of worldwide COPD situation. Proceedings of Data Analytics and Management: ICDAM 2022. 2023 Mar 25:391-405.

[29]. Agrawal A, Arora R, Arora R, Agrawal P. Applications of artificial intelligence and internet of things for detection and future directions to fight against COVID-19. InEmerging Technologies for Battling Covid-19: Applications and Innovations 2021 Feb 16 (pp. 107-119). Cham: Springer International Publishing.

[30]. Dalal S, Jaglan V, Agrawal A, Kumar A, Joshi SJ, Dahiya M. Navigating urban congestion: Optimizing LSTM with RNN in traffic prediction. InAIP Conference Proceedings 2024 Dec 20 (Vol. 3217, No. 1, p. 030005). AIP Publishing LLC.

[31]. Dalal, S., Lilhore, U. K., Simaiya, S., Prakash, D., Yadav, S., Kumar, K., & Kaushik, A. (2026). GenAD-SM: optimized transformer-VAE model for precision anomaly detection for smart manufacturing in industry 5.0. Journal of Intelligent Manufacturing, 1-21. https://doi.org/10.1007/s10845-025-02764-5

[32]. 2025

[33]. Bhutani, M., Dalal, S., Alhussein, M., Lilhore, U. K., Aurangzeb, K., & Hussain, A. (2025). SAD-GAN: A Novel Secure Anomaly Detection Framework for Enhancing the Resilience of Cyber-Physical Systems. Cognitive Computation, 17.0(4), 127.

[34]. Dalal, S., Dahiya, N., Kundu, S., Verma, A., Devi, G., Ayadi, M., Dubale, M., & Hashmi, A. (2025).

GAN-CSA: Enhanced Generative Adversarial Networks for Accurate Detection and Surgical Guidance in Skull Base Brain Metastases. International Journal of Computational Intelligence Systems, 18.0(1), 310.

[35]. Dalal, S., Lilhore, U. K., Faujdar, N., Simaiya, S., Agrawal, A., Rani, U., & Mohan, A. (2025). Enhancing thyroid disease prediction with improved XGBoost model and bias management techniques. Multimedia Tools and Applications, 84.0(16), 16757-16788.

[36]. Dalal, S., Lilhore, U. K., Seth, B., Radulescu, M., & Hamrioui, S. (2025). A Hybrid Model for Short-Term Energy Load Prediction Based on Transfer Learning with LightGBM for Smart Grids in Smart Energy Systems. Journal of Urban Technology, 32.0(1), 49-75.

[37]. Kaur, N., Mittal, A., Lilhore, U. K., Simaiya, S., Dalal, S., Saleem, K., & Ghith, E. S. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP Journal on Wireless Communications and Networking, 2025.0(1), 5.

[38]. Lilhore, U. K., Dalal, S., Radulescu, M., & Barbulescu, M. (2025). Smart grid stability prediction model using two-way attention based hybrid deep learning and MPSO. Energy Exploration & Exploitation, 43.0(1), 142-168.

[39]. Lilhore, U. K., Simaiya, S., & Dalal, S. (2025). 10 Hybrid Mathematical Optimization Techniques in AI. Math Optimization for Artificial Intelligence: Heuristic and Metaheuristic Methods for Robotics and Machine Learning, 2.0, 223.

[40]. Lilhore, U. K., Simaiya, S., Alhussein, M., Dalal, S., Aurangzeb, K., & Hussain, A. (2025). An Attention-Driven Hybrid Deep Neural Network for Enhanced Heart Disease Classification. Expert Systems, 42.0(2), e13791.

[41]. Lilhore, U. K., Simaiya, S., Dalal, S., & Faujdar, N. (2025). Revolutionizing air quality forecasting: Fusion of state-of-the-art deep learning models for precise classification. Urban Climate, 59.0, 102308.

[42]. Lilhore, U. K., Simaiya, S., Dalal, S., Alshuhail, A., & Almusharraf, A. (2025). A Post-Quantum Hybrid Encryption Framework for Securing Biometric Data in Consumer Electronics. IEEE Transactions on Consumer Electronics.

[43]. Lilhore, U. K., Simaiya, S., Dalal, S., Radulescu, M., & Balsalobre-Lorente, D. (2025). Intelligent waste sorting for sustainable environment: A hybrid deep learning and transfer learning model. Gondwana Research, 146.0, 252-266.

[44]. Malik, N., Kalonia, A., Dalal, S., & Le, D. N. (2025). Optimized XGBoost Hyper-Parameter Tuned Model with Krill Herd Algorithm (KHA) for Accurate Drinking Water Quality Prediction. SN Computer Science, 6.0(3), 263.

[45]. Ritika, R., Chhillar, R. S., Dalal, S., Moorthi, I., Dubale, M., & Hashmi, A. (2025). Enhanced heart disease diagnosis and management: A multi-phase framework leveraging deep learning and personalized nutrition. PLoS One, 20.0(10), e0334217.

[46]. Yadav, S., Sehrawat, H., Jaglan, V., Singh, S., Kantha, P., Goyal, P., & Dalal, S. (2025). A Novel Effective Forecasting Model Developed Using Ensemble Machine Learning For Early Prognosis of Asthma Attack and Risk Grade Analysis. Scalable Computing: Practice and Experience, 26.0(1), 398-414.

